Oeson
Inspiring generation

DHCP using HYENAE

Developed By Wilson Canete Kamacupa

Oeson
Inspiring generation

Agenda

1. PROJECT OBJECTIVE
2. PROJECT REQUIREMENT
3. DHCP INTRODUCTION AND CONFIGURATION
4. INTRODUCTION OF HYENAE TOOL
5. INSTALLATION STEPS FOR HYENAE IN WINDOWS
6. DHCP ATTACK USING HYENAE
7. CONCLUSION
8. REFERENCE

Oeson
Inspiring generation

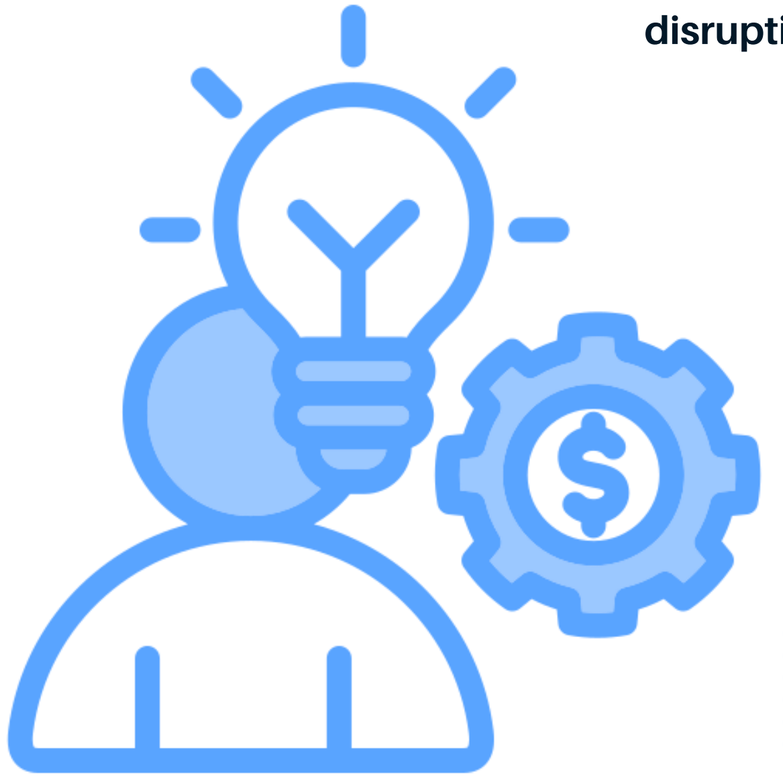
Warning

1. The information provided in this presentation is intended for educational purpose only.
2. Unauthorized scanning or exploitation of system is illegal and unethical.
3. Always obtain proper authorization before conducting any security assessments.

Oeson
Inspiring generation

Project Objective

The objective of this project is to demonstrate a DHCP starvation attack using Hyenae tool, a network packet generator. This attack will target a Windows Server DHCP service, simulating a real-world scenario where an attacker depletes available IP addresses, disrupting network operations.



Oeson
Inspiring generation

Project Requirement

Primary Host

Windows 11

Virtual Machine

Windows Server configured Bridged Adapter Network

Tool

Hyenae (hyenae Advanced Network Evaluator) will be used for generating and manipulating packets on the network

Oeson
Inspiring generation

DHCP Introduction and Configuration

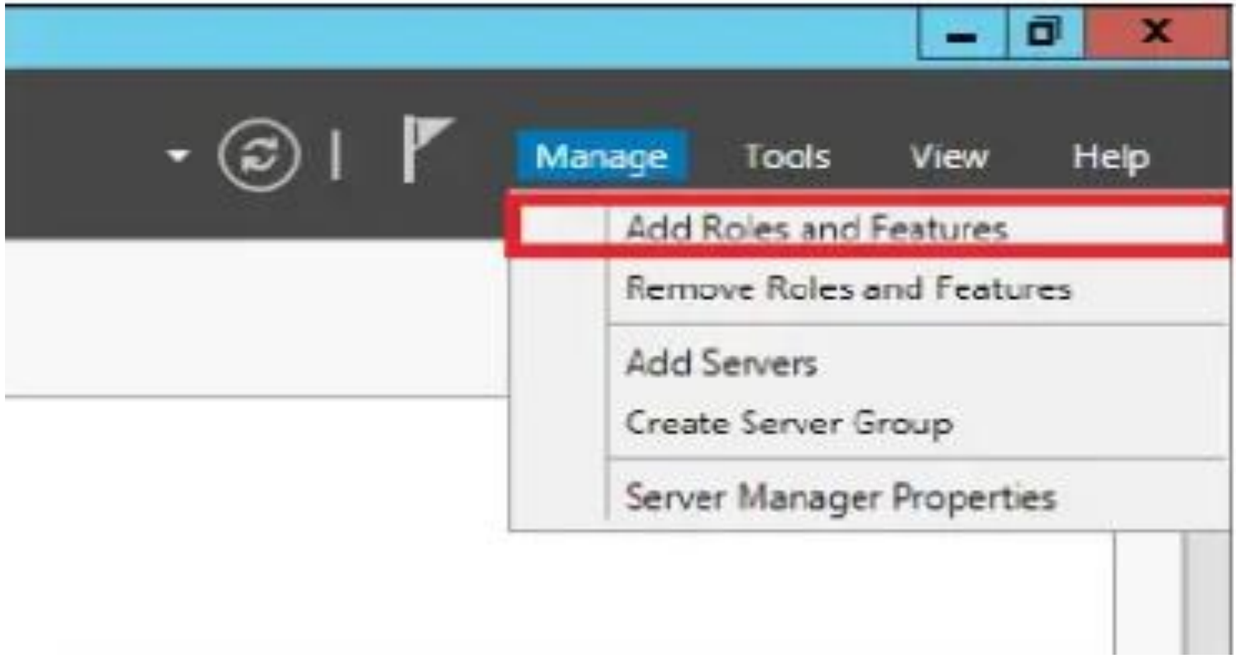
DHCP (Dynamic Host Configuration Protocol)

Is a network protocol used to automatically assign IP addresses and other configuration parameters to devices on a network. It simplifies the process of setting up and managing IP addresses by dynamically allocating them as devices connect to the network. This is especially useful in larger networks where manual IP address configuration would be time-consuming and error-prone.

Oeson
Inspiring generation

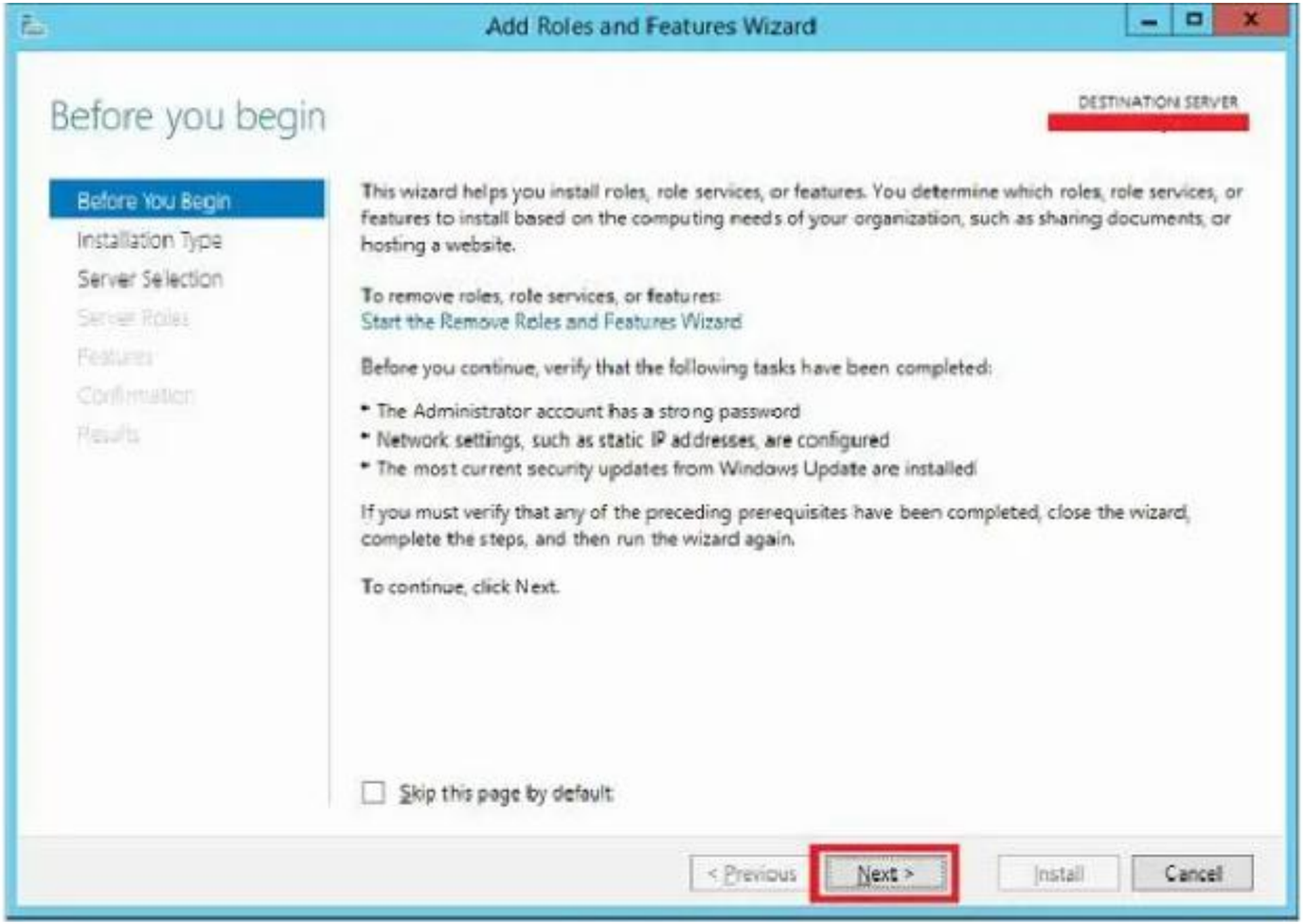
To install DHCP in Windows Server you will have to follow the steps given below

Step 1 - Go to “Server Manager” → Manager → Add Roles and Features



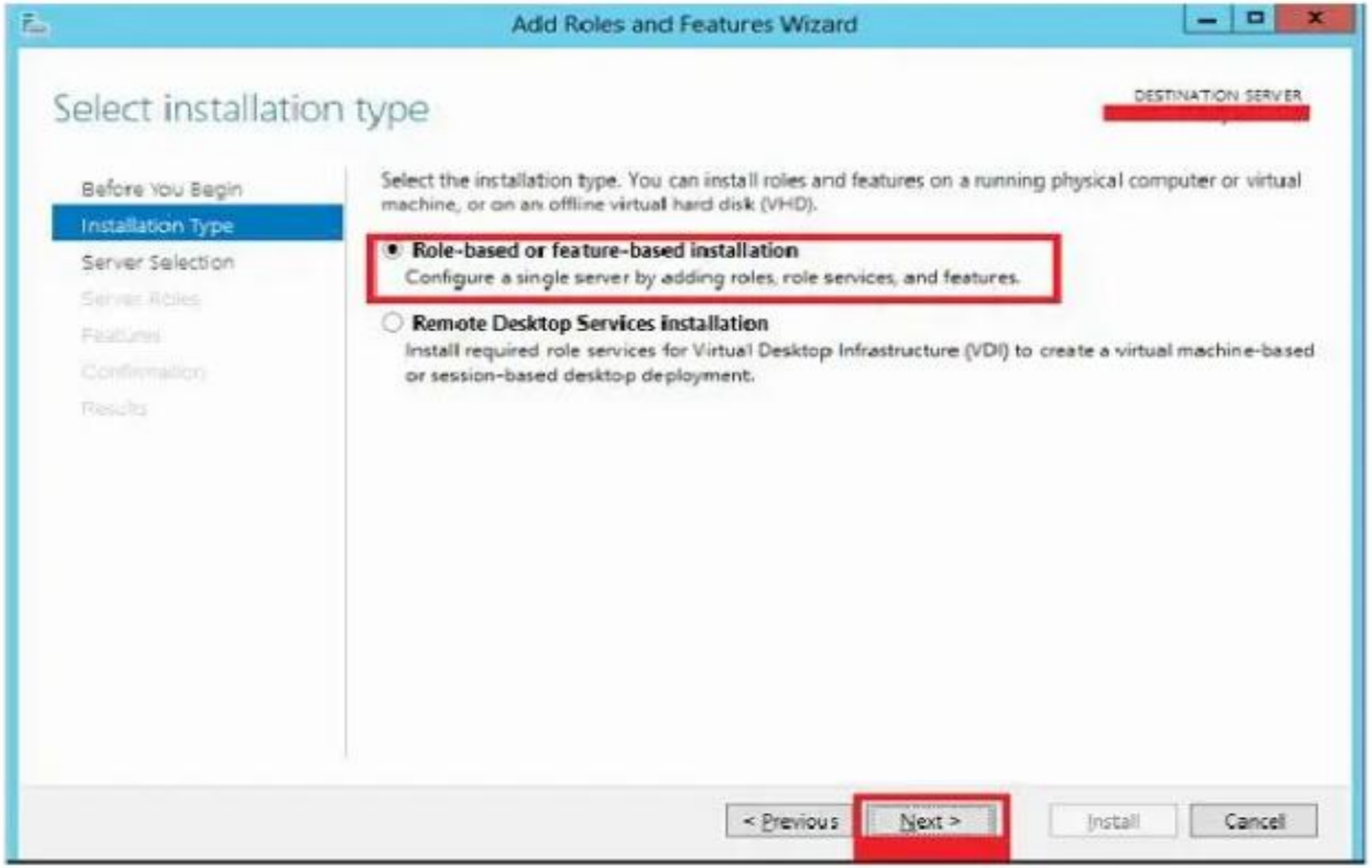
Oeson
Inspiring generation

Step 2 - Click Next



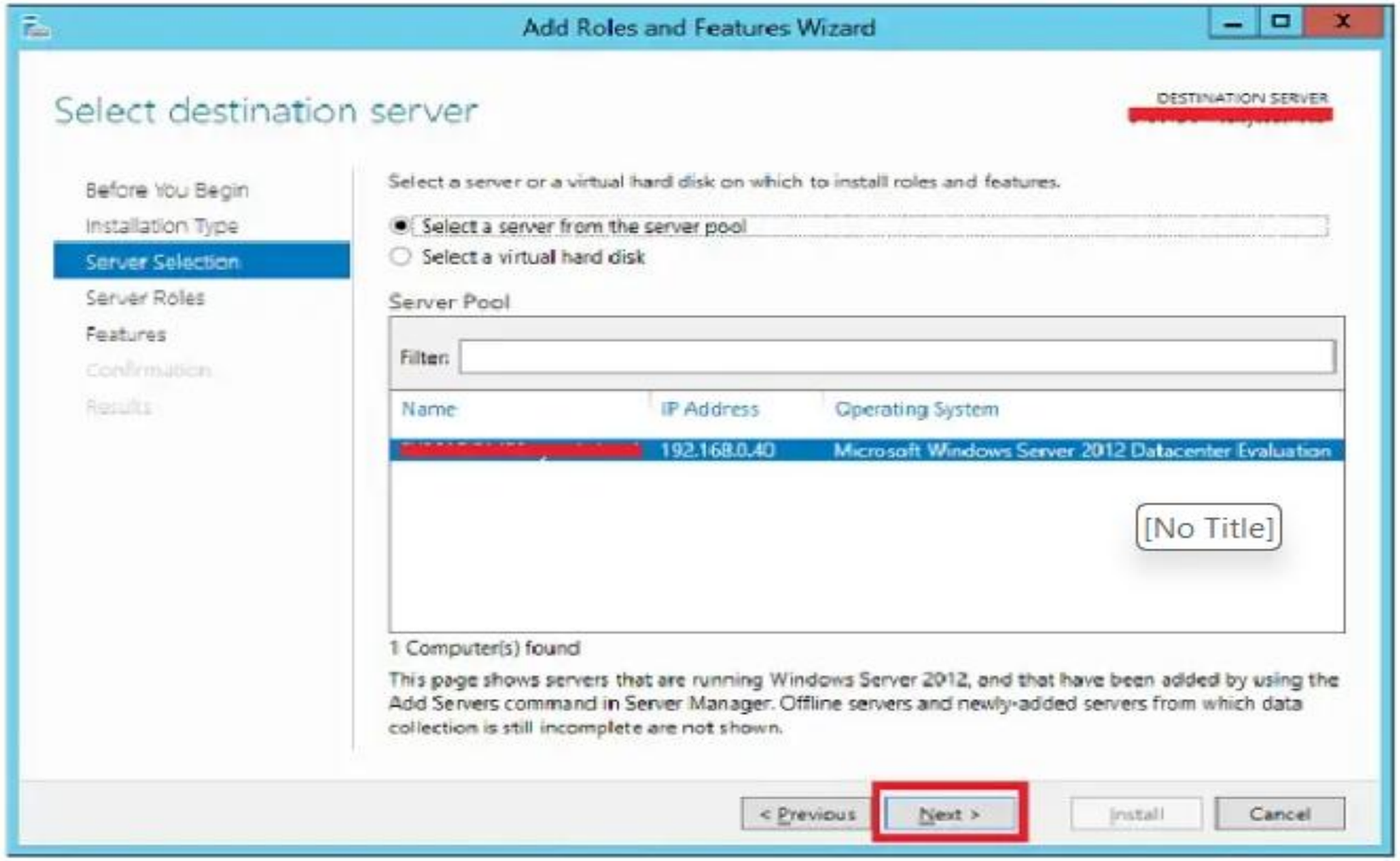
Oeson
Inspiring generation

Step 3 – Select the Role-based or feature-based installation option → click Next



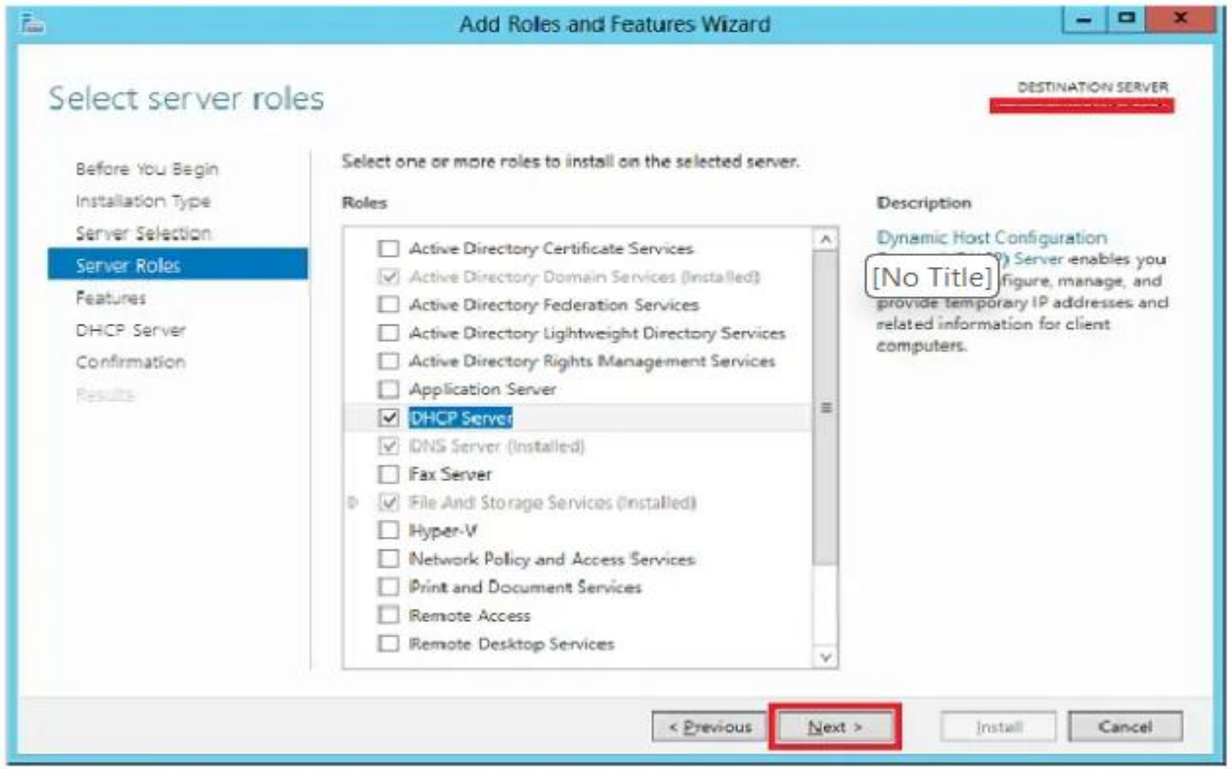
Oeson
Inspiring generation

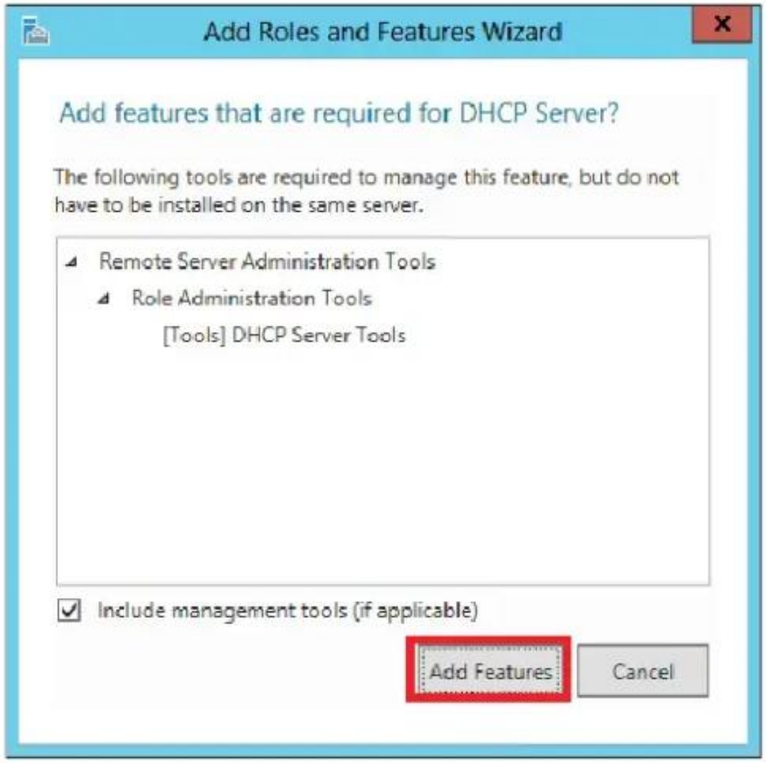
Step 4 – We will install a Local DHCP Role as it will select a server from the Server pool → click Next



Oeson
Inspiring generation

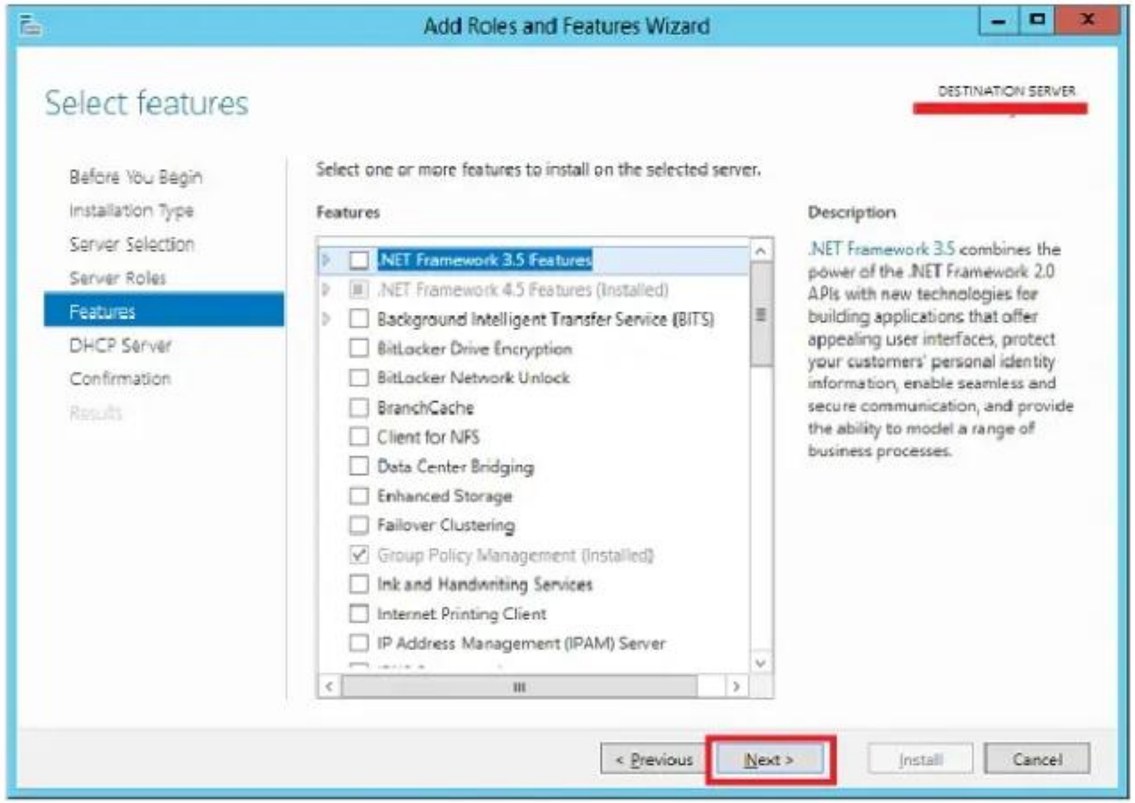
Step 5 – From the Roles lists, check the DHCP Server role → click Add Features on the popup windows as shown in the following screenshots

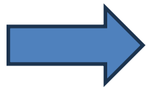


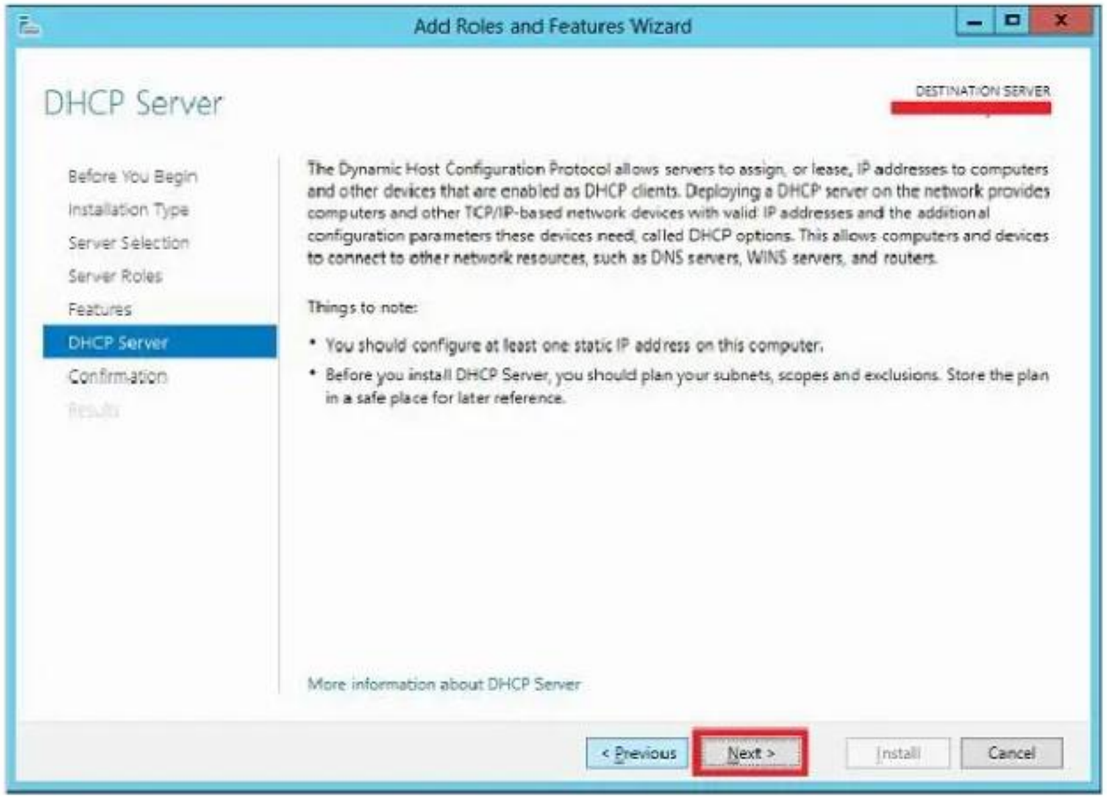


Oeson
Inspiring generation

Step 6 - Click Next

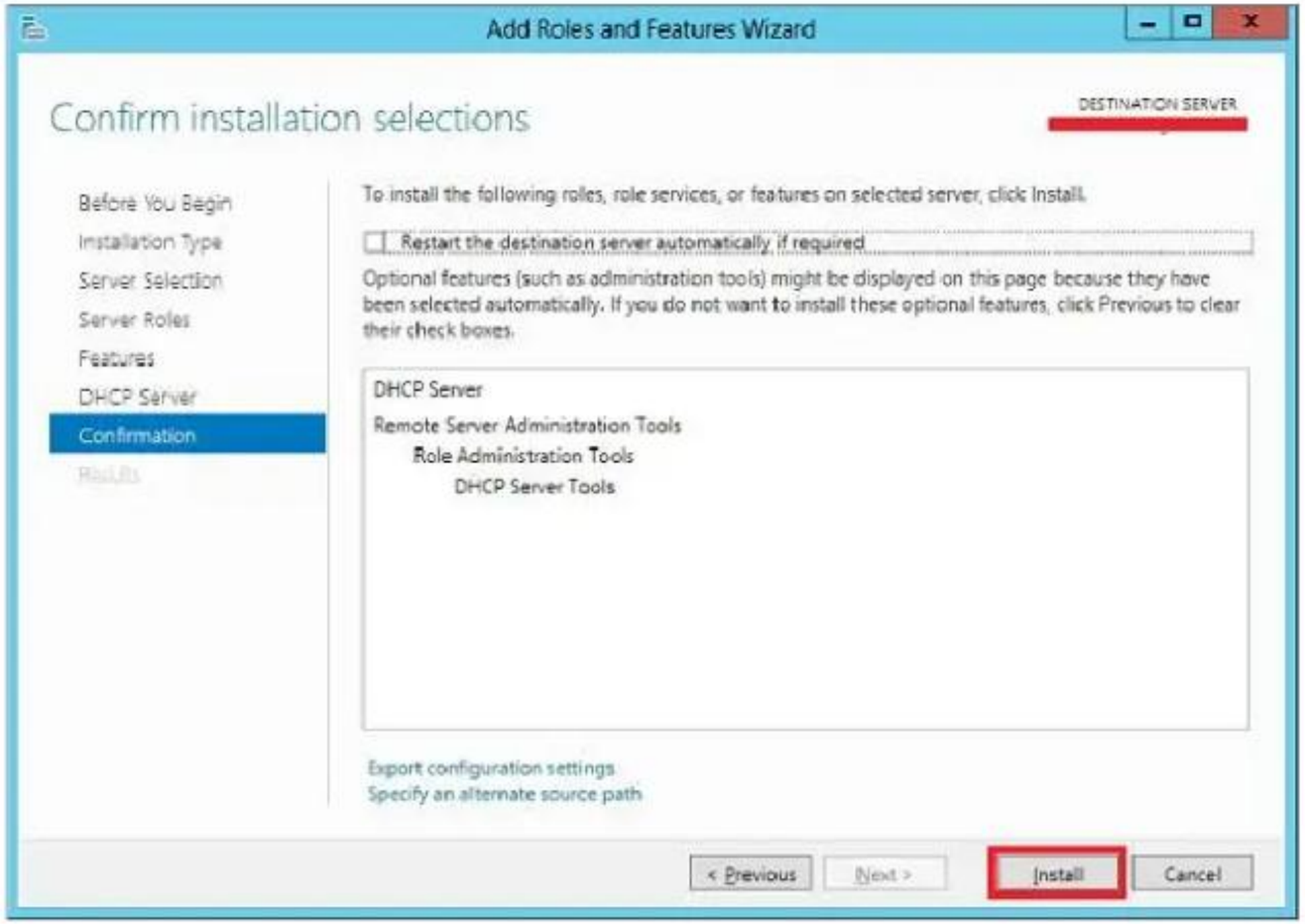






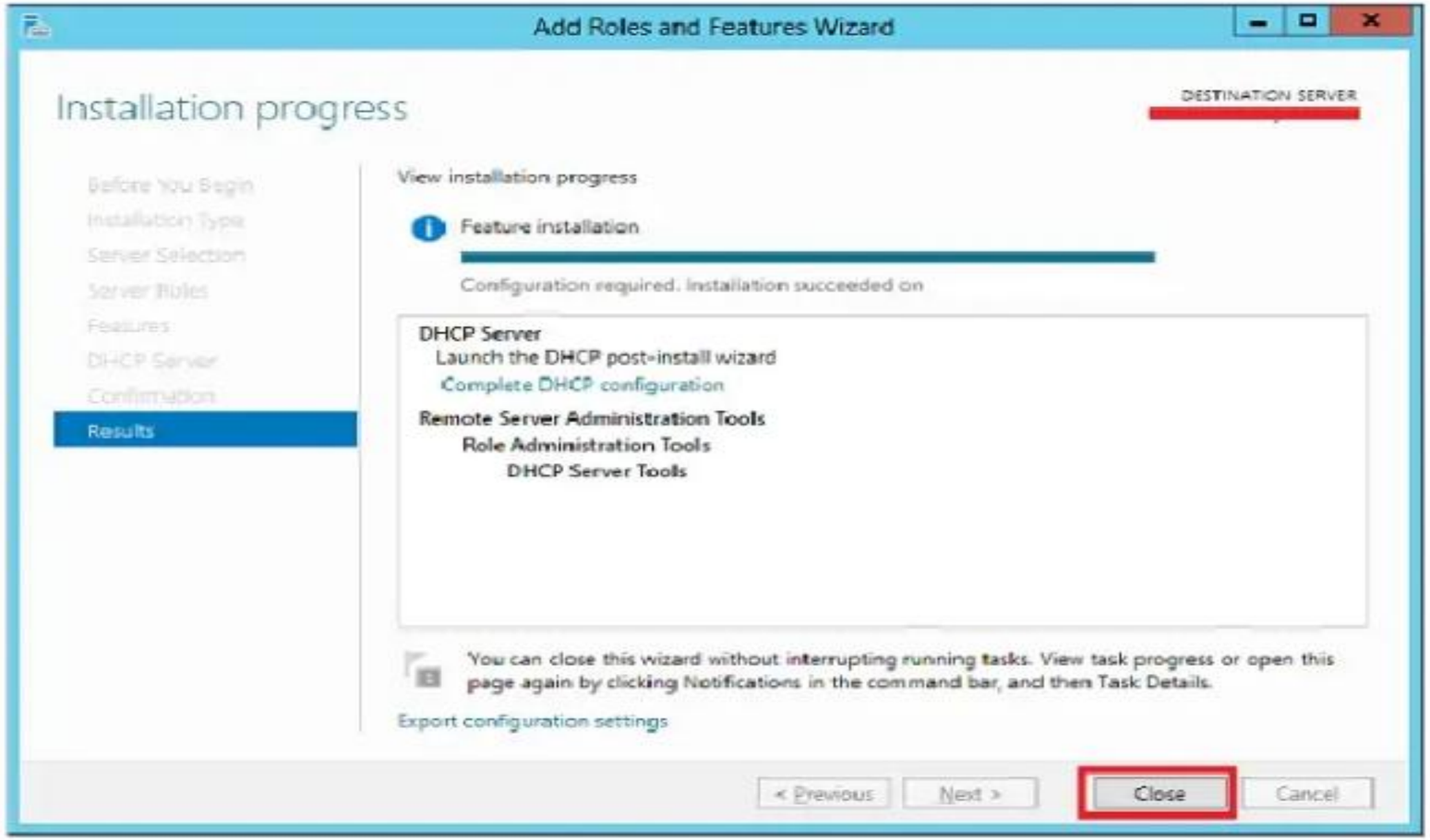
Oeson
Inspiring generation

Step 7 – Click Install



Oeson
Inspiring generation

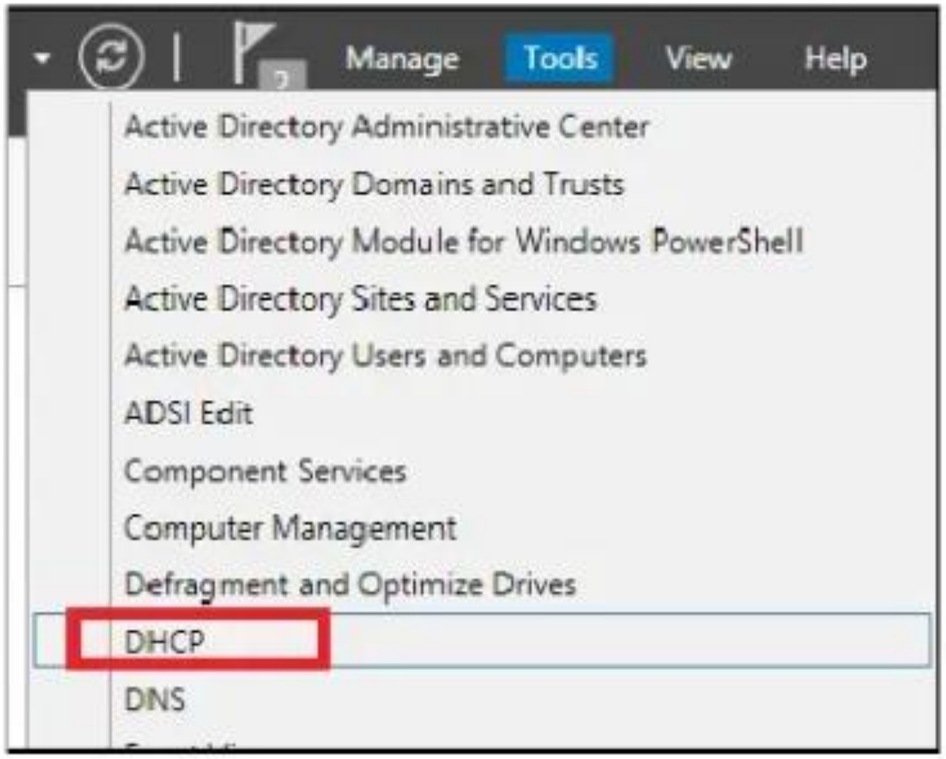
Step 8 - Click close



Oeson
Inspiring generation

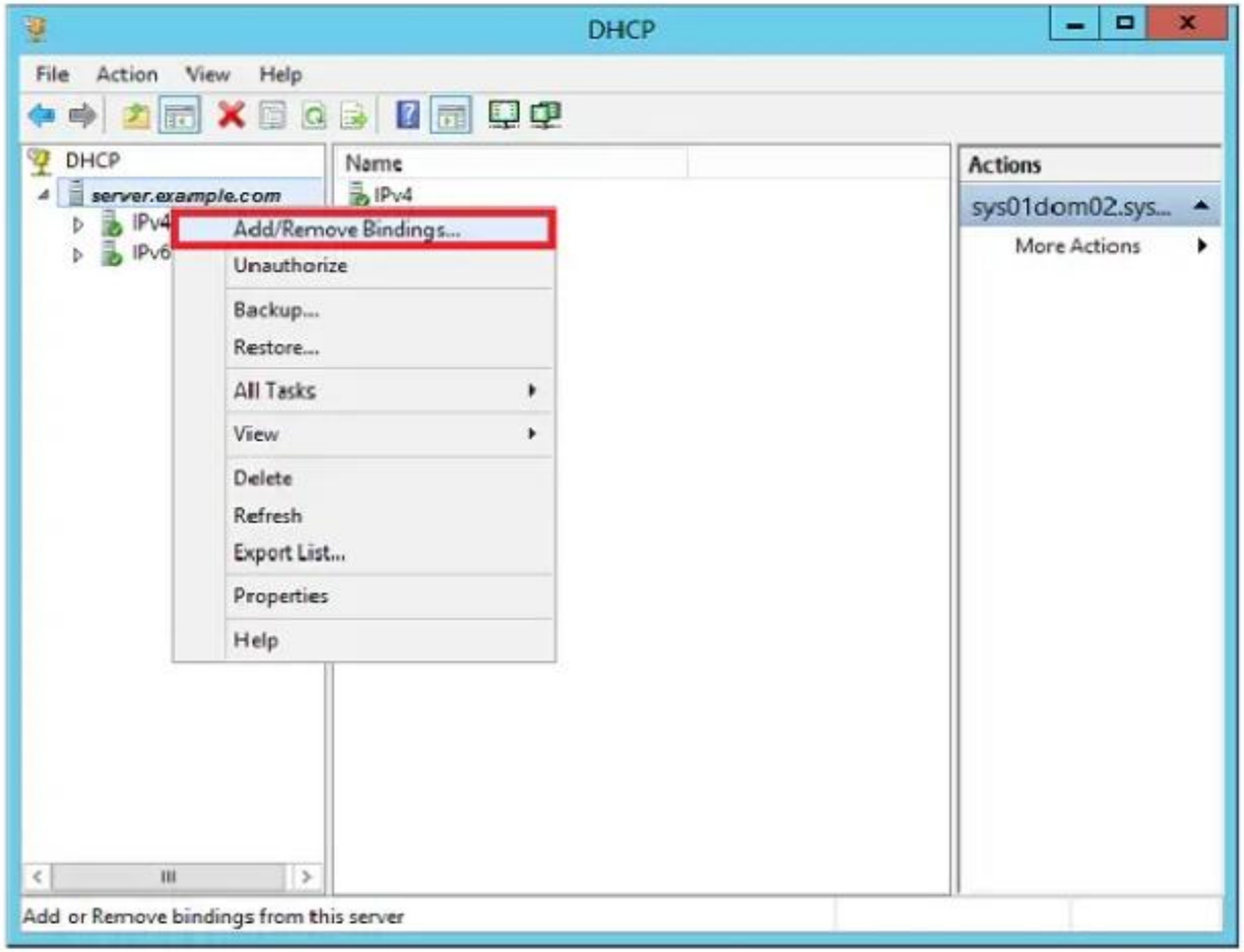
Now we have to configure the service to make it useful for the computers. To do this, we need to follow the steps given below

Step 1 - Server Manager screen → Tools → DHCP



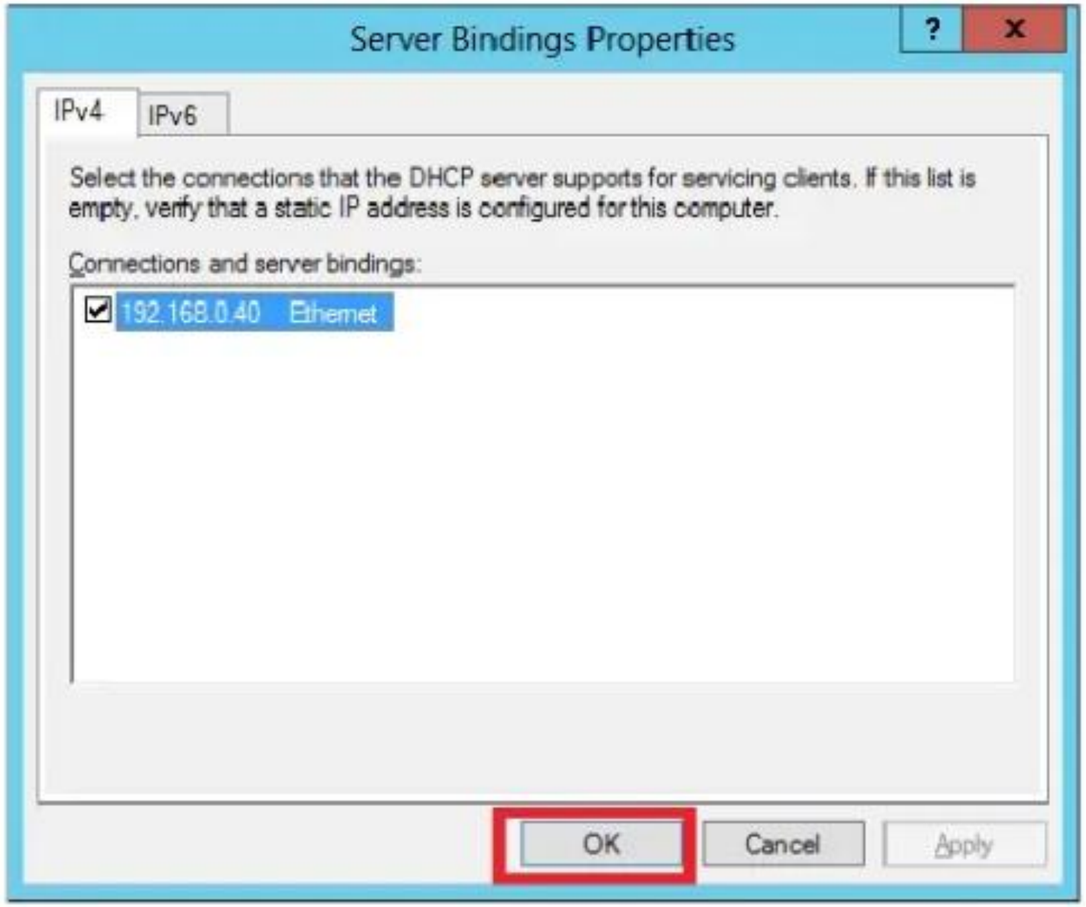
Oeson
Inspiring generation

Step 2 – Right click on the DHCP Server → then click on “Add/Remove Bindins…”



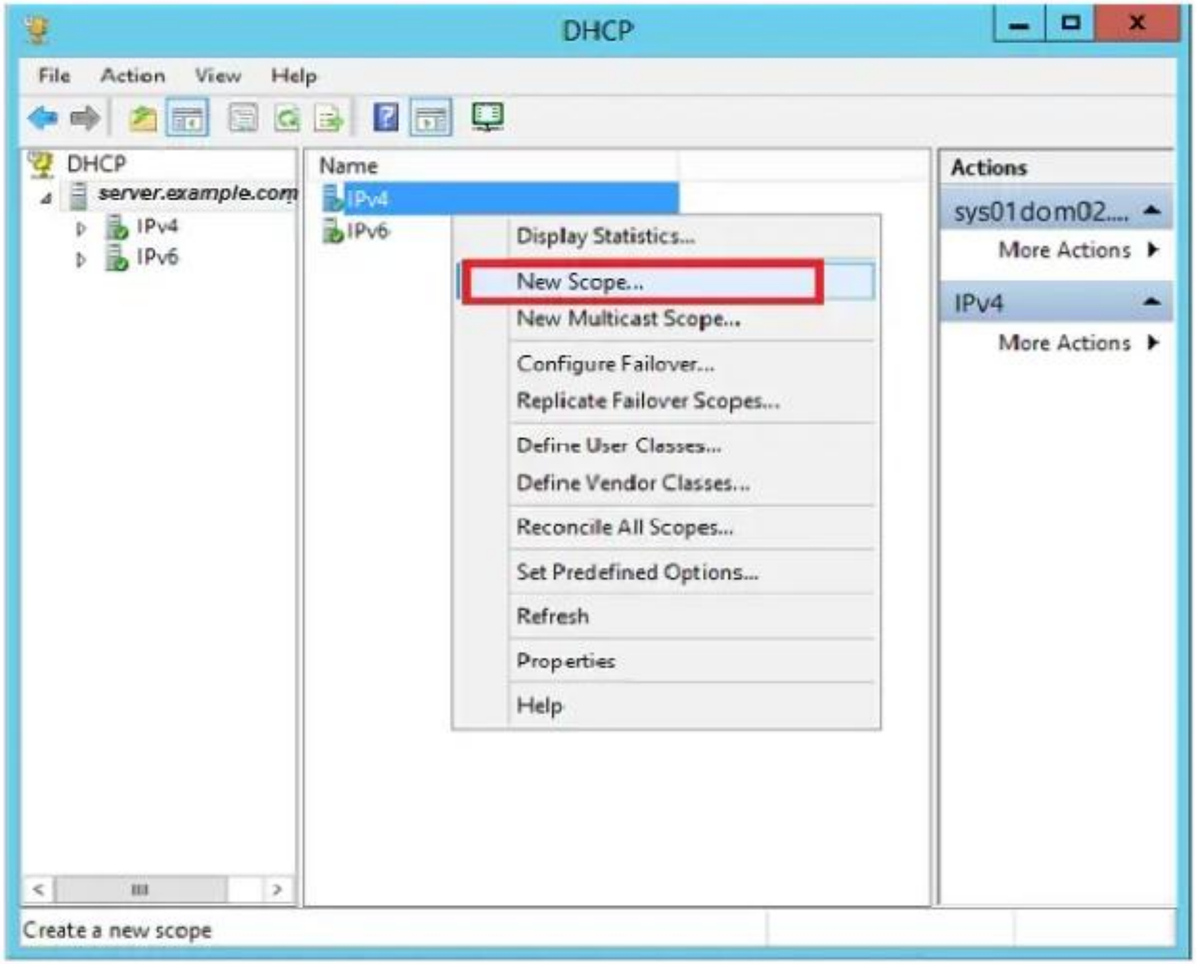
Oeson
Inspiring generation

Step 3 - Ensure the static IP address of the server should appear as shown in the following screenshot



Oeson
Inspiring generation

Step 4 – Right click on IPv4 → Select “New Scope”

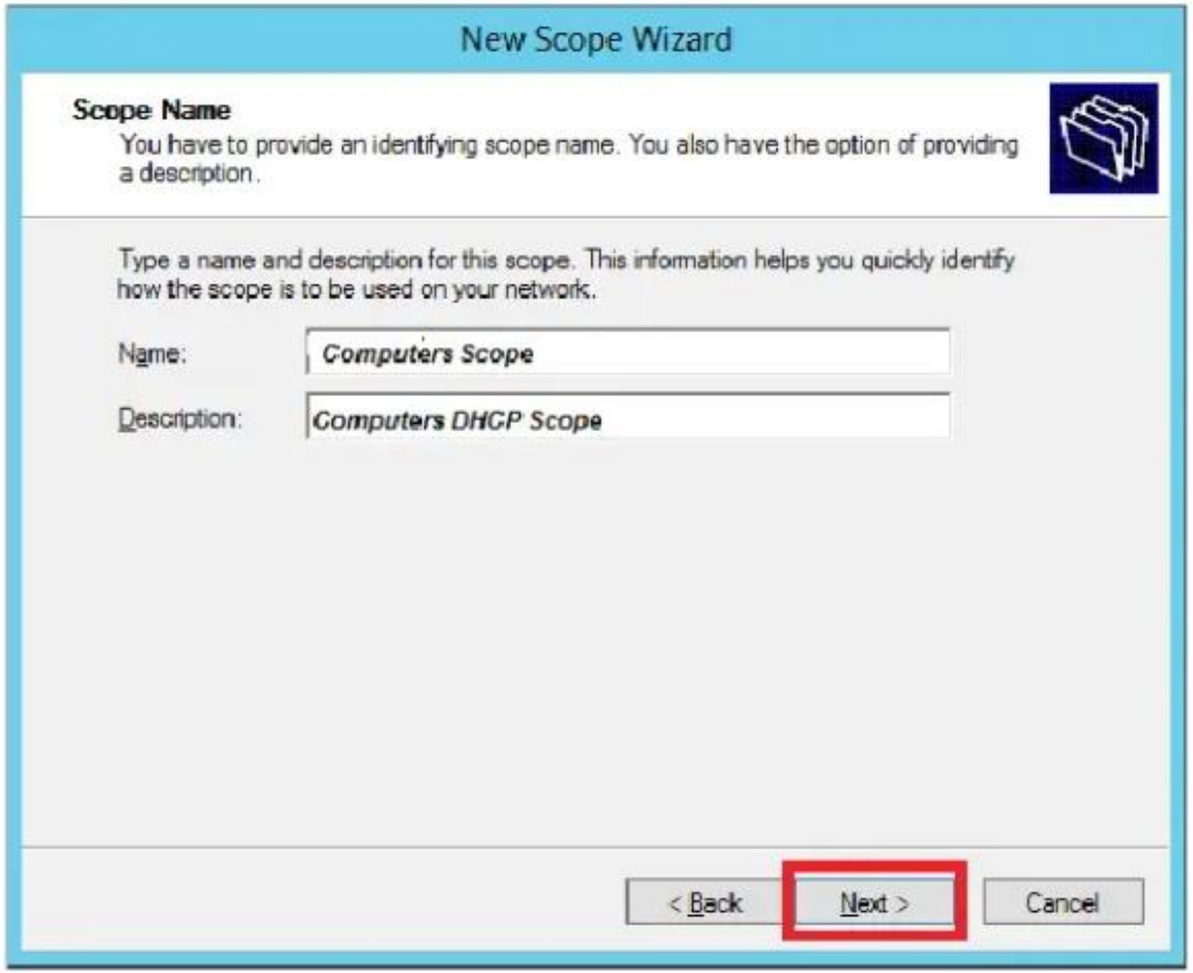


Oeson
Inspiring generation

Step 5 - Click Next

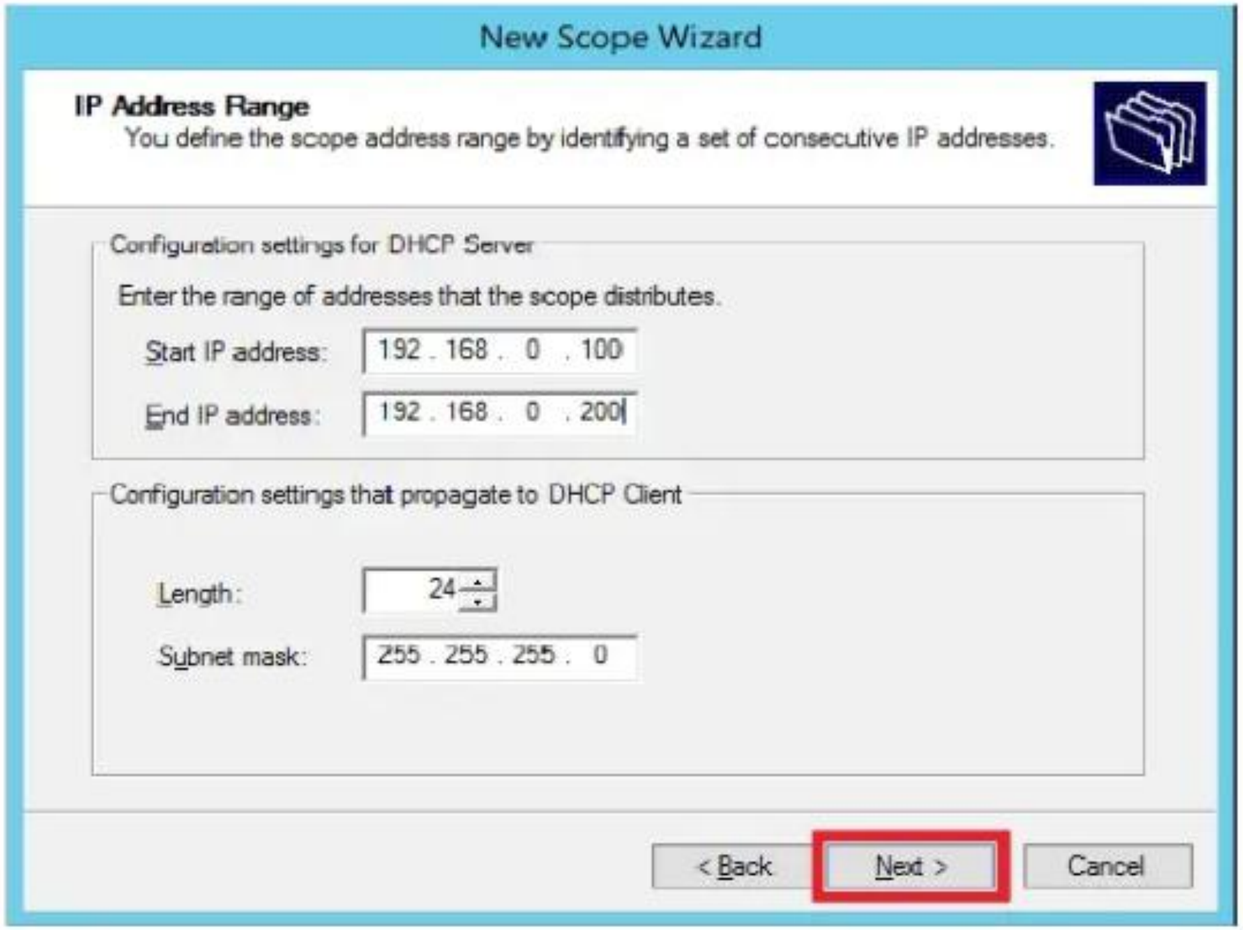
Oeson
Inspiring generation

Step 6 – Enter Scope Name and Description as shown in the following screeshot and then → Next



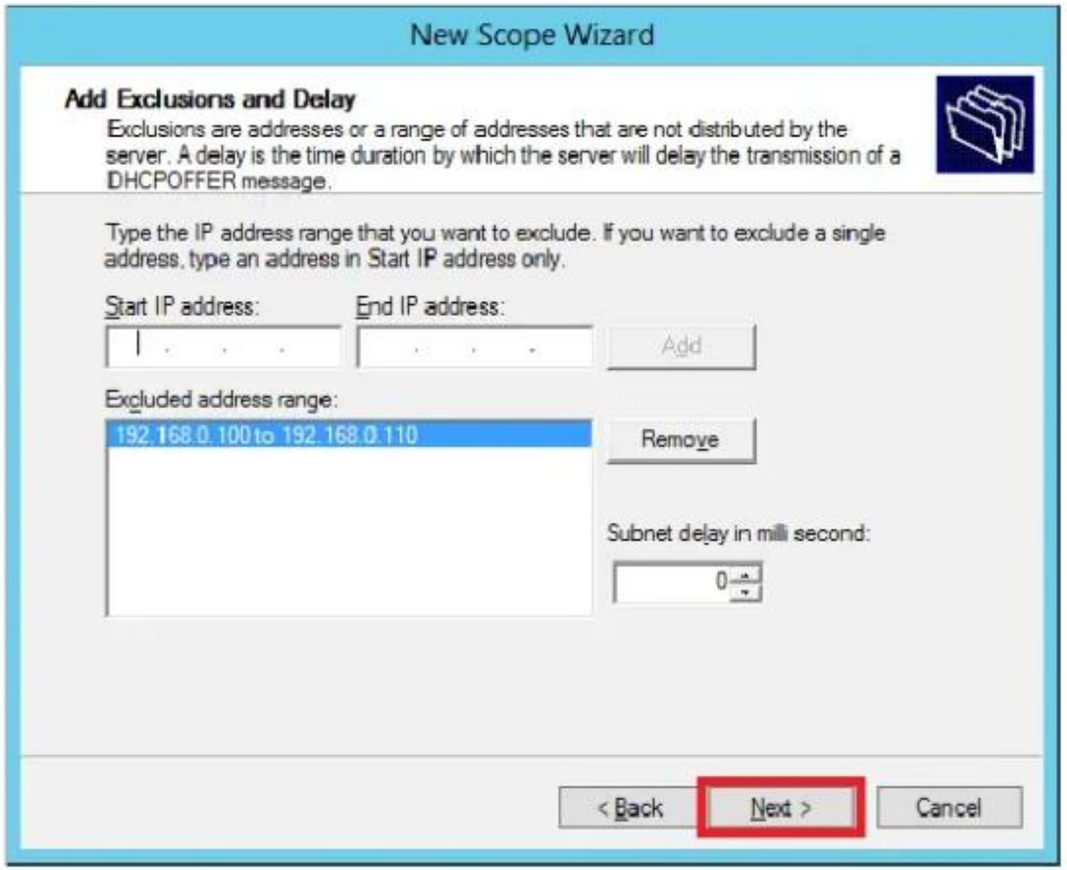
Oeson
Inspiring generation

Step 7 – Enter the Start and End IP address, the Subnet mask, leave the Length as default “24” for class C subnet → click Next



Oeson
Inspiring generation

Step 8 - Enter your IP range in the exclusion list, if you have devices on the network that require static IP address and also ensure that the excluded range falls with the Start and End range earlier specified, then → click Next

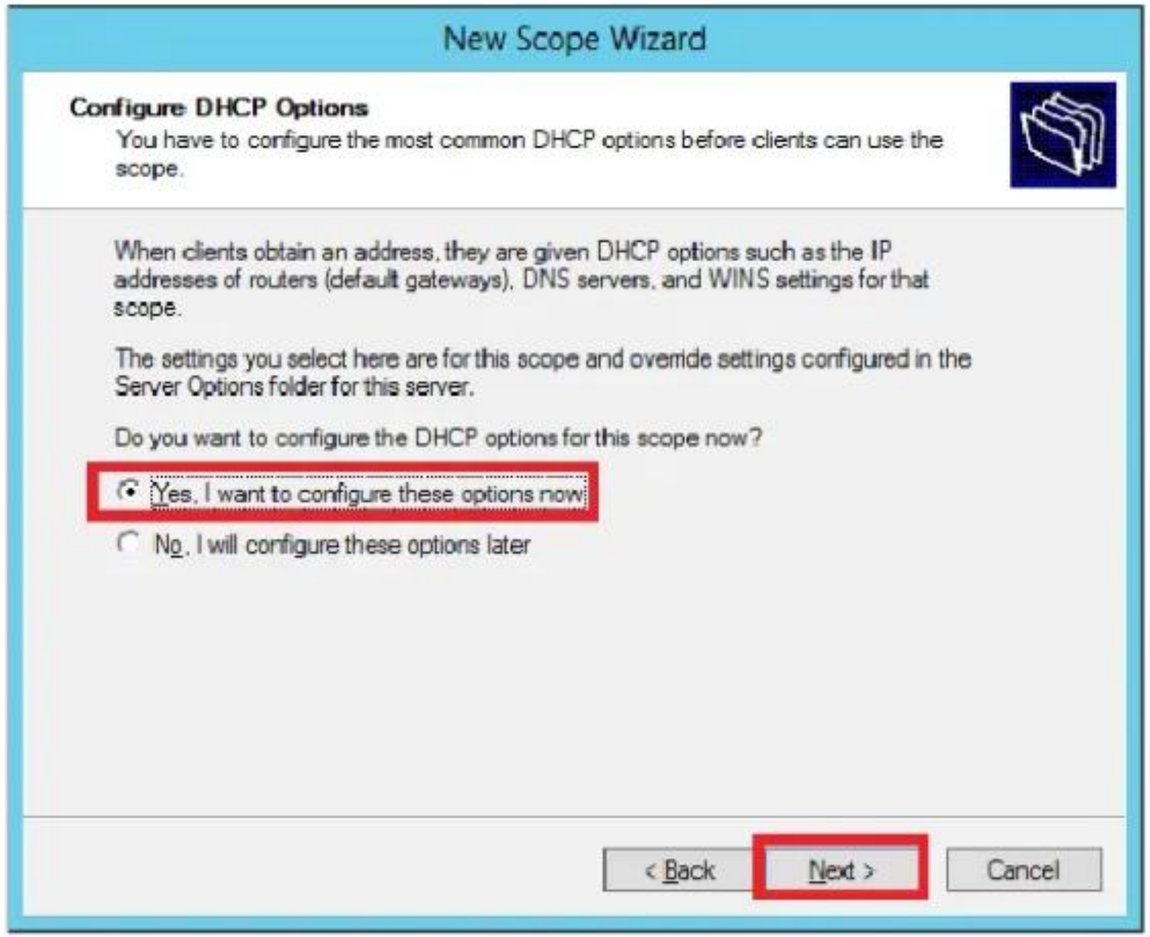


Oeson
Inspiring generation

Step 9 - Enter the desired lease duration for the assigned IP's or leave as default → then click Next

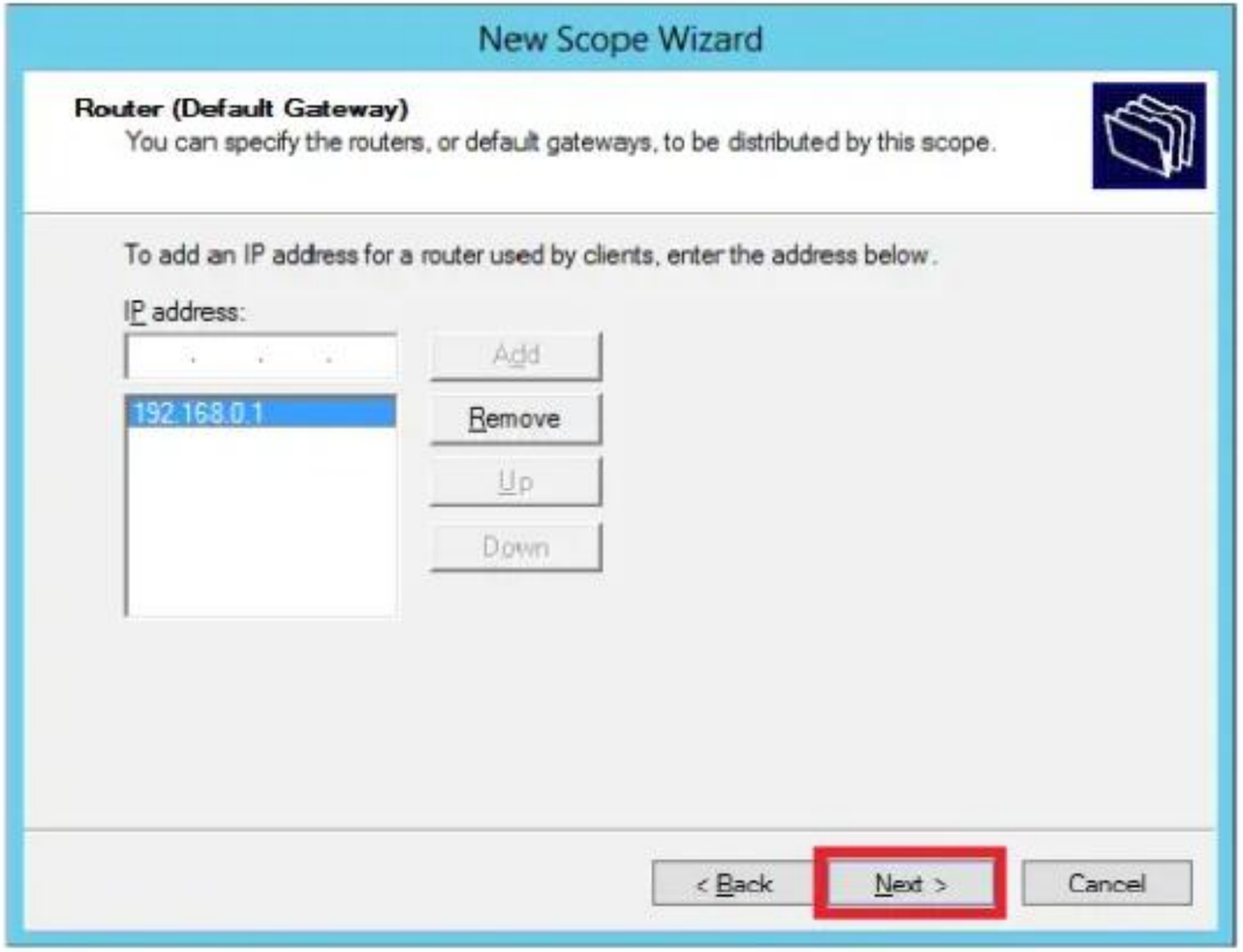
Oeson
Inspiring generation

Step 10 – Select → Yes, I want to configure these option now to configure the DHCP options for the new scope → then click on Next



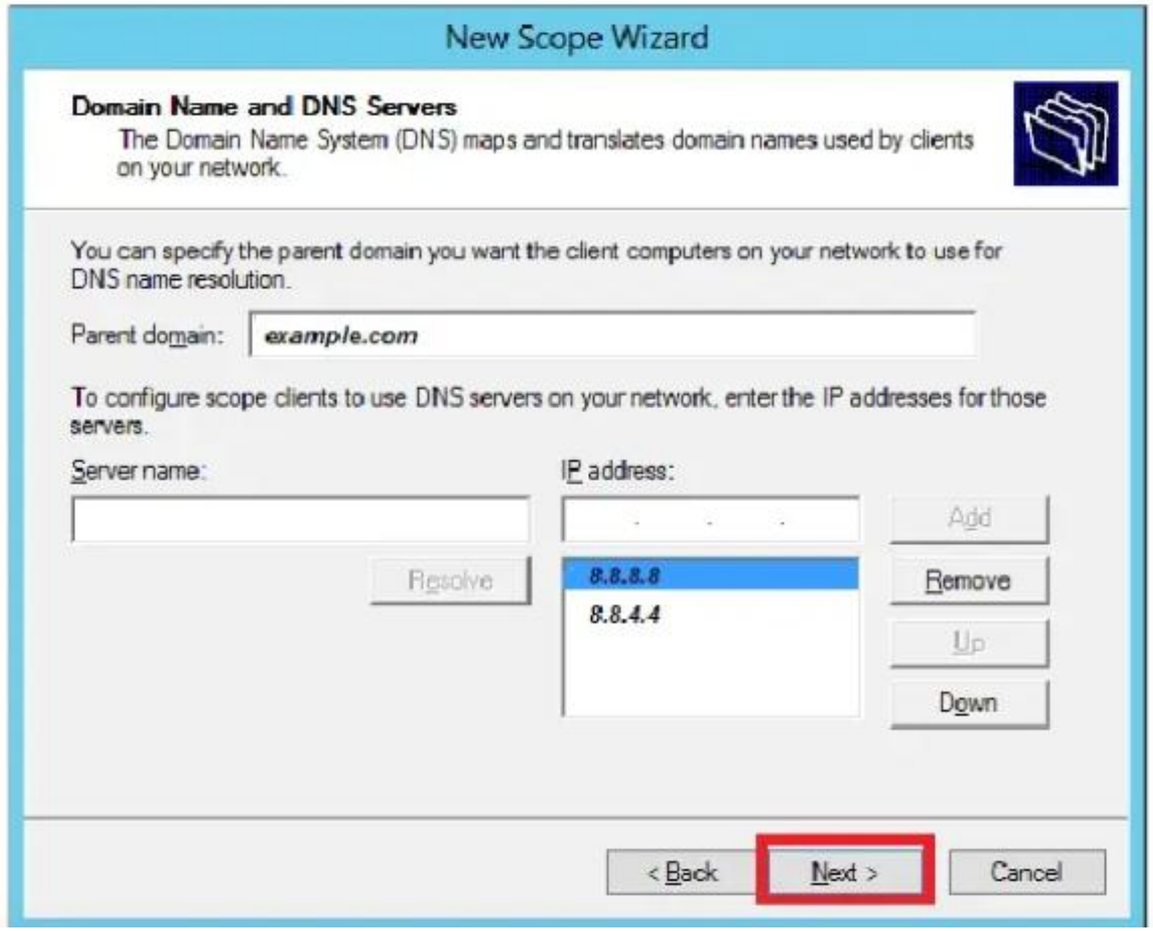
Oeson
Inspiring generation

Step 11 - Enter the default gateway which is the IP of your Router → Then click Next



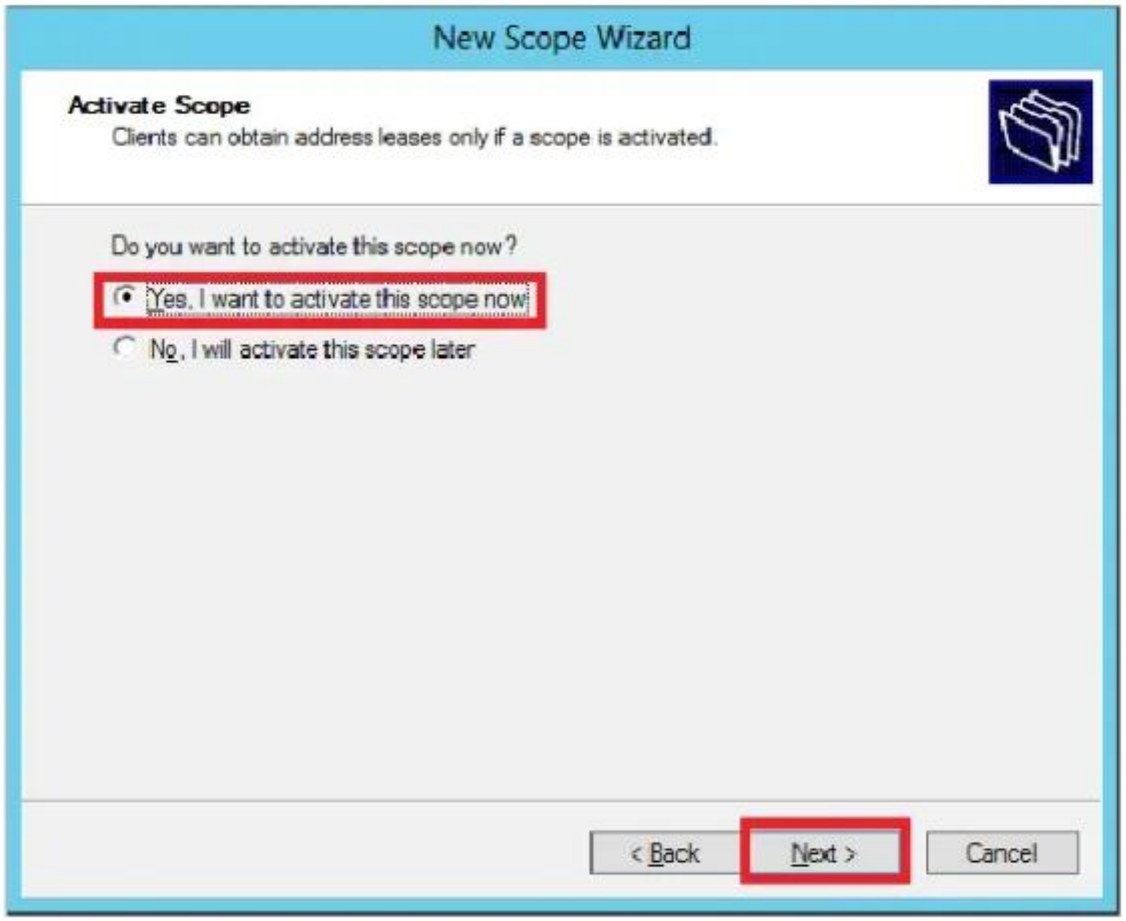
Oeson
Inspiring generation

Step 12- Add DNS IP → click Next (we can put Google DNS or if it is a Domain environment you can put the DC IP there) then click → Next



Oeson
Inspiring generation

Step 13 – select “Yes, I want to activate this scope now”option to activate the scope immediately and then click → Next



Oeson
Inspiring generation

Step 14 - Click finish

Oeson
Inspiring generation

Introduction of Hyenae tool

Hyenae

Hyenae is a highly flexible platform independent network packet generator. It allows you to reproduce several MITM, DoS and DDoS attack scenarios, comes with a clusterable remote daemon and an interactive attack assistant.

Hyenae is a free software published in other list of programs, part of System Utilities.

It is available in English and is compatible with the different operating systems, such as Linux and others.

Oeson
Inspiring generation

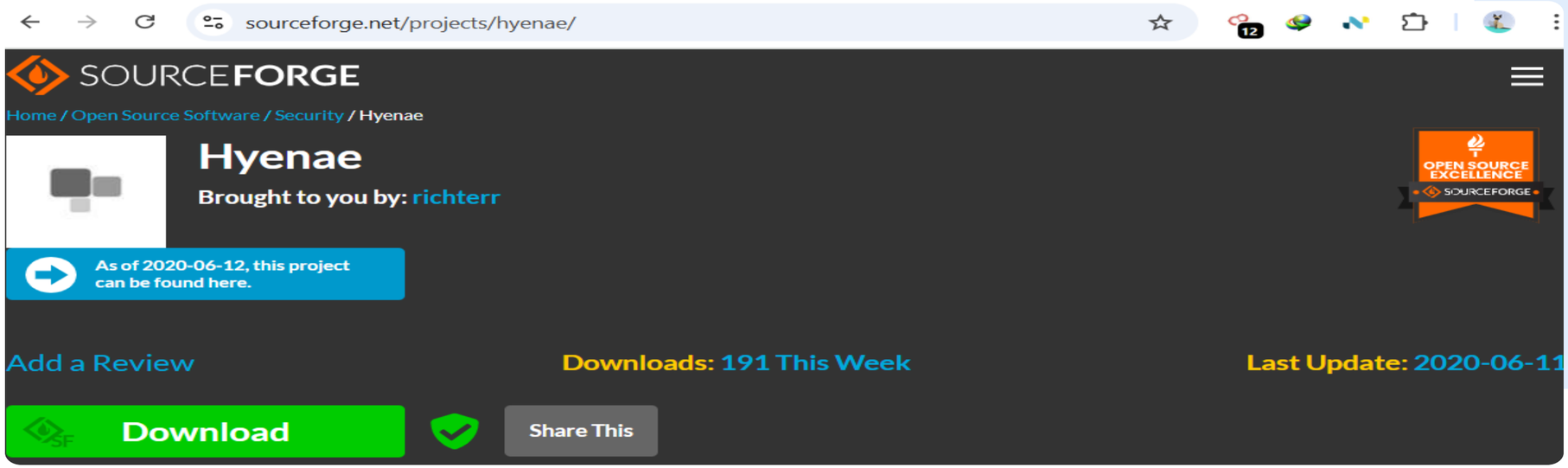
Installation step for Hyenae in Windows System

As a versatile network packet generator that supports various attack simulations, including DHCP-related scenarios. To install Hyenae on a Windows system, follow the steps below:

1. Download Hyenae:

- Visit the official SourceForge page to download the latest Windows version of Hyenae:

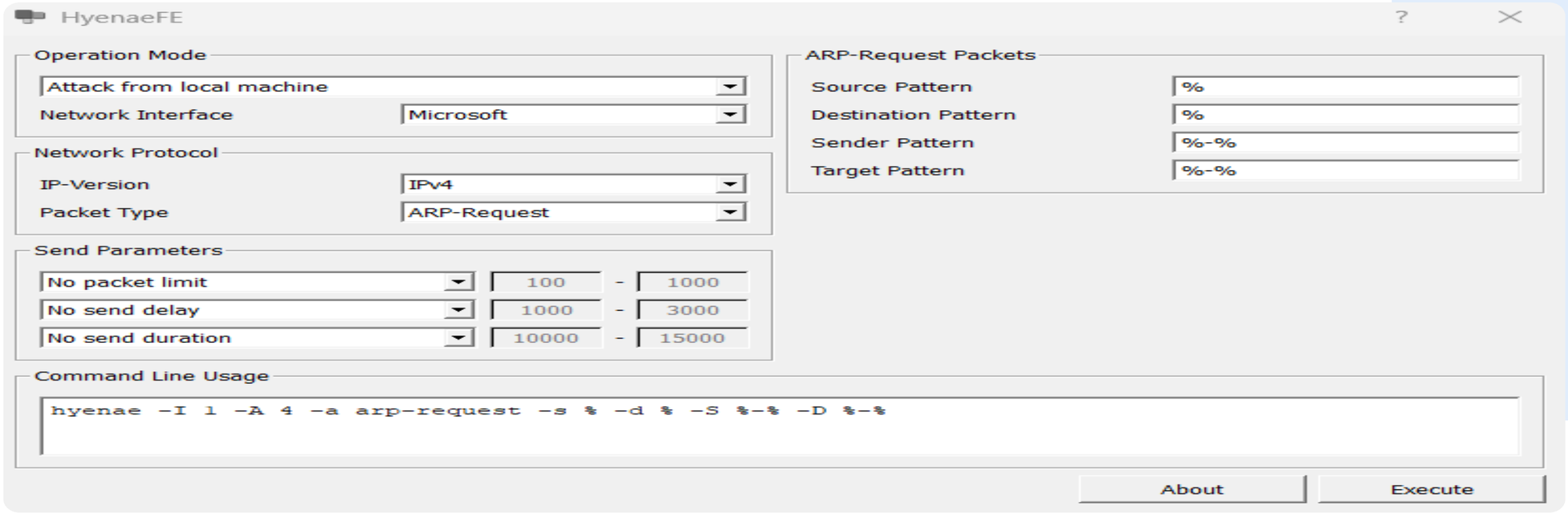
  https://sourceforge.net/projects/hyenae/



Oeson
Inspiring generation

2. Install Hyenae:

- Locate the downloaded Hyenae executable file .
- Double-click the file to run the installer.
- Follow the installation prompts:
  - Choose the components to install.
  - Choose the destination folder for installation.
  - Confirm and complete the installation process.



Oeson
Inspiring generation

DHCP Attack using Hyenae

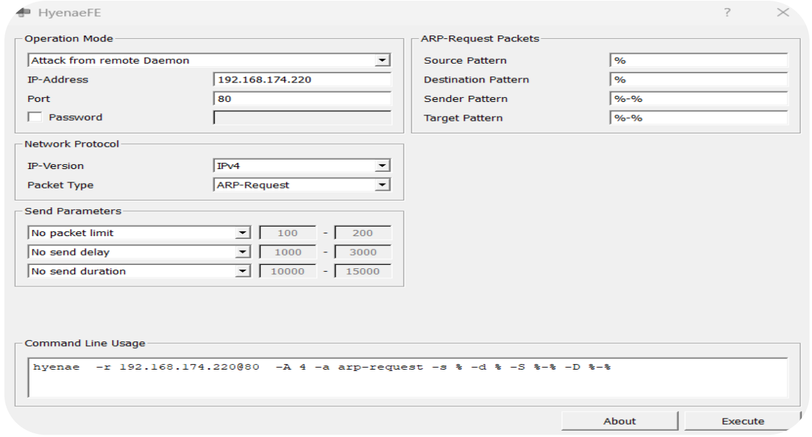
In this agenda I will explain how to perform a DHCP starvation attack from a Windows machine (host) targeting a Windows Server VM running as a DHCP server.

1 — 2 — 3

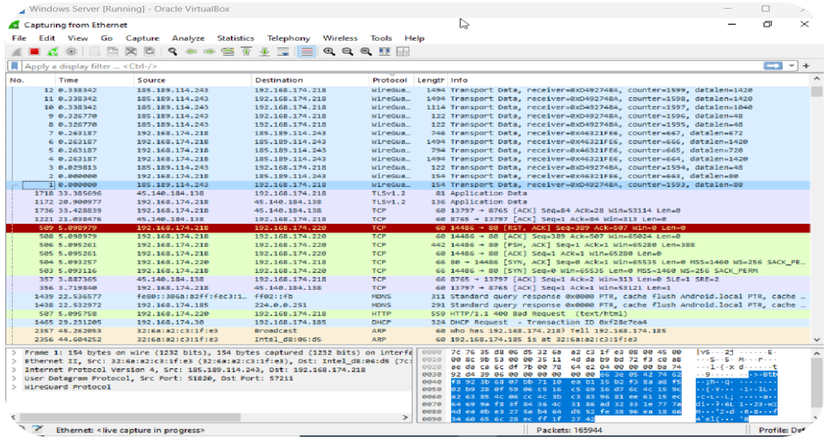
Before starting testing with Hyenae, make sure your primary Windows can communicate with your Windows Server:

```
C:\Windows\System32>ping 192.168.174.220

Pinging 192.168.174.220 with 32 bytes of data:
Reply from 192.168.174.220: bytes=32 time=4ms TTL=128
Reply from 192.168.174.220: bytes=32 time=6ms TTL=128
Reply from 192.168.174.220: bytes=32 time=3ms TTL=128
Reply from 192.168.174.220: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.174.220:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

start training with Hyenae by sending malicious packets to Windows Server.

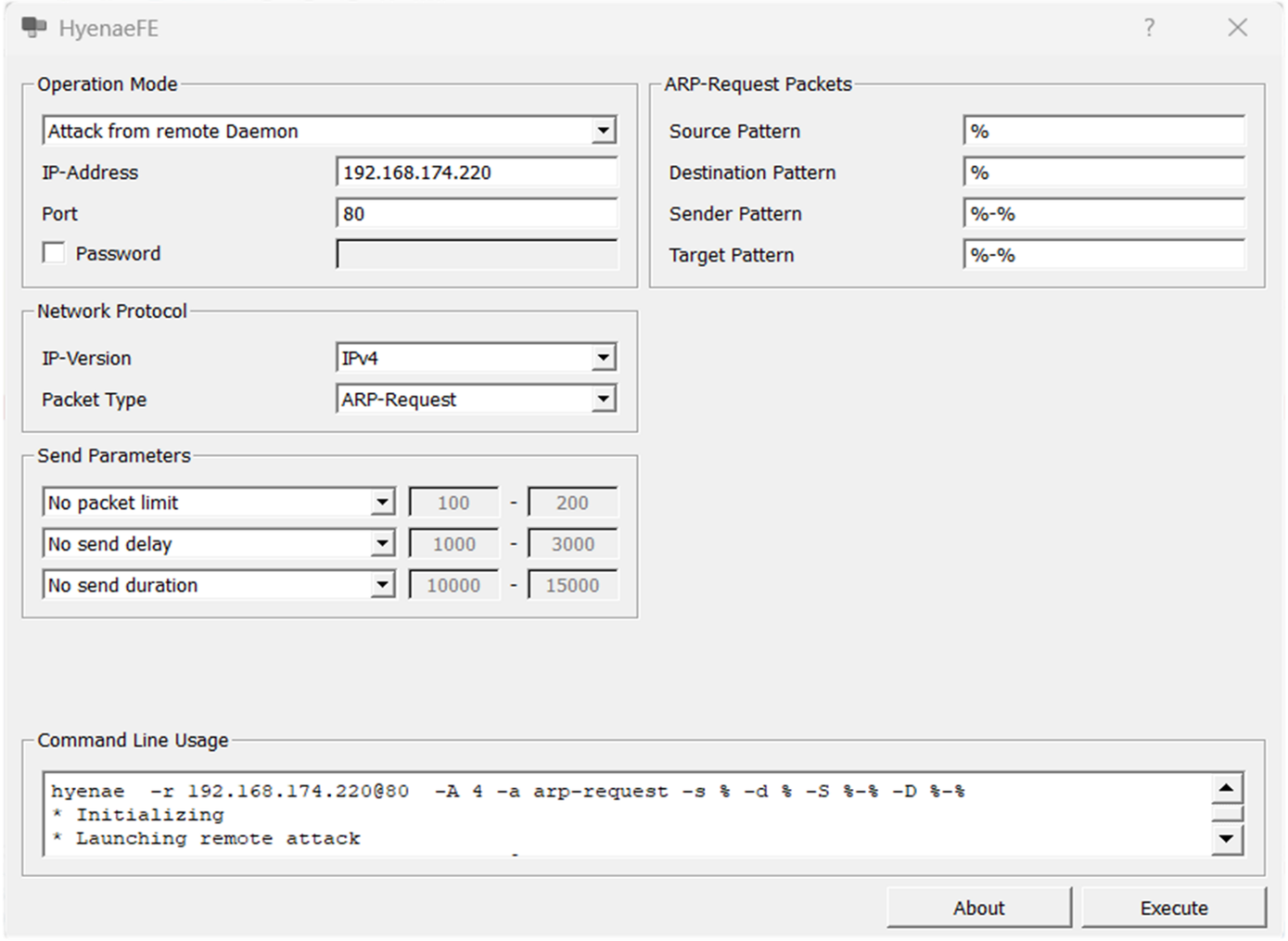


Wireshark on Windows Server to view packets being sent



Oeson
Inspiring generation

View packets being sent



The image show an attempted remote ARP attack using Hyenae, where:

Operation Mode:

The attack via remote Daemon (Hyenae background service) was selected.

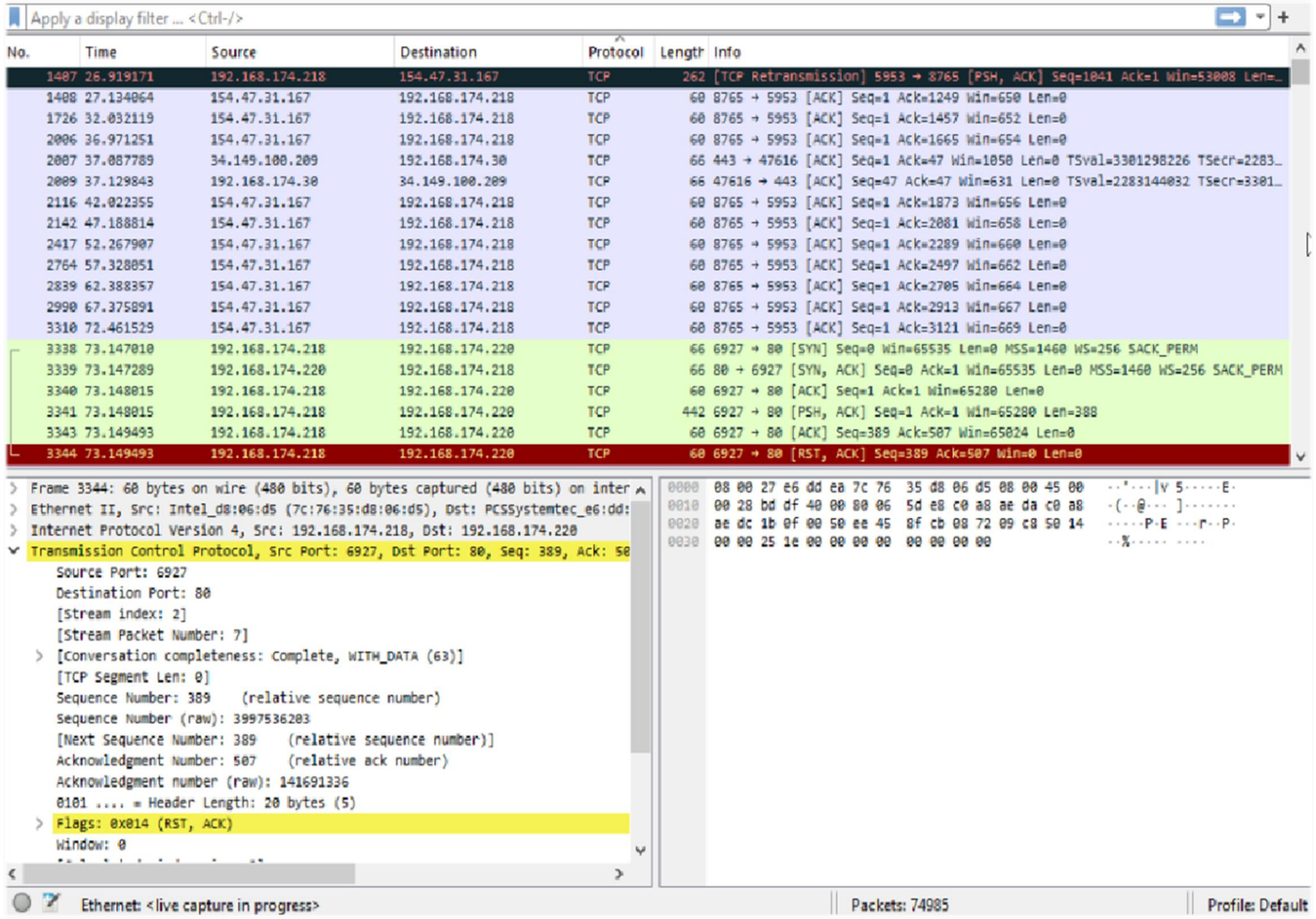
The target is Windows Server with IP 192.168.174.220, with port 80.

Protocol Configuration:

Protocol: IPv4 with ARP-Request type packets (used for spoofing or ARP poisoning attacks).

Oeson
Inspiring generation

Start training with Hyenae by sending malicious packets to Windows Server.



The screenshot image show a complete TCP handshake between IP 192.168.174.218 (primary host) and 192.168.174.220 (Windows server on port 80), starting with a SYN from the primary host (port 6927), followed by a SYN-ACK from the server and an acknowledgement ACK (packets 3338-3340). After establishing the connection, the primary host send data (388-byte PSH,ACK in packet 3341) and ends with an acknowledgement ACK (3343) and a possible abnormal termination (LSI,ACK in packet 3344, which would normally be FIN,ACK to close the connection properly). The pattern indicates a normal HTTP communication, but with an abnormal termination.

Oeson
Inspiring generation

Conclusion

This project aimed to demonstrate a DHCP starvation attack using the Hyenae tool, simulating a real-world scenario where an attacker exhausts the available IP addresses on a DHCP server, causing disruptions to network operations.

The Hyenae tool was not effective on Windows 11 as a primary system, which is believed to have been better on Kali Linux.

In summary, this project highlighted the need to protect critical network services, such as DHCP, from malicious exploits, reinforcing the importance of cybersecurity awareness and best practices.

Oeson
Inspiring generation

References

- dhcp-protocol. (2025). Retrieved from portnox.com: https://www.portnox.com/cybersecurity-101/dhcp-protocol/
- hyenae. (2020, 06 24). Retrieved from github.com: https://github.com/r-richter/hyenae
- Protocolo DHCP. (2024, 11 02). Retrieved from learn.microsoft.com: https://learn.microsoft.com/pt-br/windows-server/networking/technologies/dhcp/dhcp-top

THANK YOU!

wilsoncanetekamacupa@gmail.com